Respuesta a Incidentes

Formas de Respuesta a Incidentes

A lo largo de este trabajo elaboraremos diversas formas de respuestas a incidentes, en concreto crearemos un “PlayBook” o guía sobre cómo responder, contener, mitigar y eliminar un incidente, en concreto un ransomware siguiendo con trabajos anteriores. Adaptaremos el trabajo a nuestro gusto y especificaremos los pasos a seguir durante el PlayBook.

CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ERIC SUAREZ VAZQUEZ

08/05/2024

1. PlayBook

1.1. ¿Qué es un PlayBook? ¿Para qué sirve?

Si hablamos en términos coloquiales, en español un "**playbook**" podría **compararse** con un libro de instrucciones detallado por un **cuerpo técnico**, donde se describen las distintas **estrategias** o **acciones** a implementar para minimizar los **daños**.

Definición: Es una guía estratégica que detalla las acciones a seguir en respuesta a eventos específicos, como incidentes de ciberseguridad.

Objetivo: Coordinar respuestas efectivas y eficientes a incidentes y situaciones de crisis.

Contenido: Protocolos, responsabilidades, procesos de comunicación, y pasos a seguir durante y después de un incidente.

Aplicación: Se utiliza principalmente en equipos de respuesta a incidentes de ciberseguridad para guiar la respuesta ante eventos de seguridad específicos.

Ejemplo: En caso de un ataque de ransomware, el playbook puede guiar al equipo sobre cómo identificar el ataque, quién debe ser notificado, cómo comunicar el incidente a los empleados, y qué pasos técnicos seguir para mitigar el daño.

1.2. ¿Qué es realmente una respuesta a incidente?

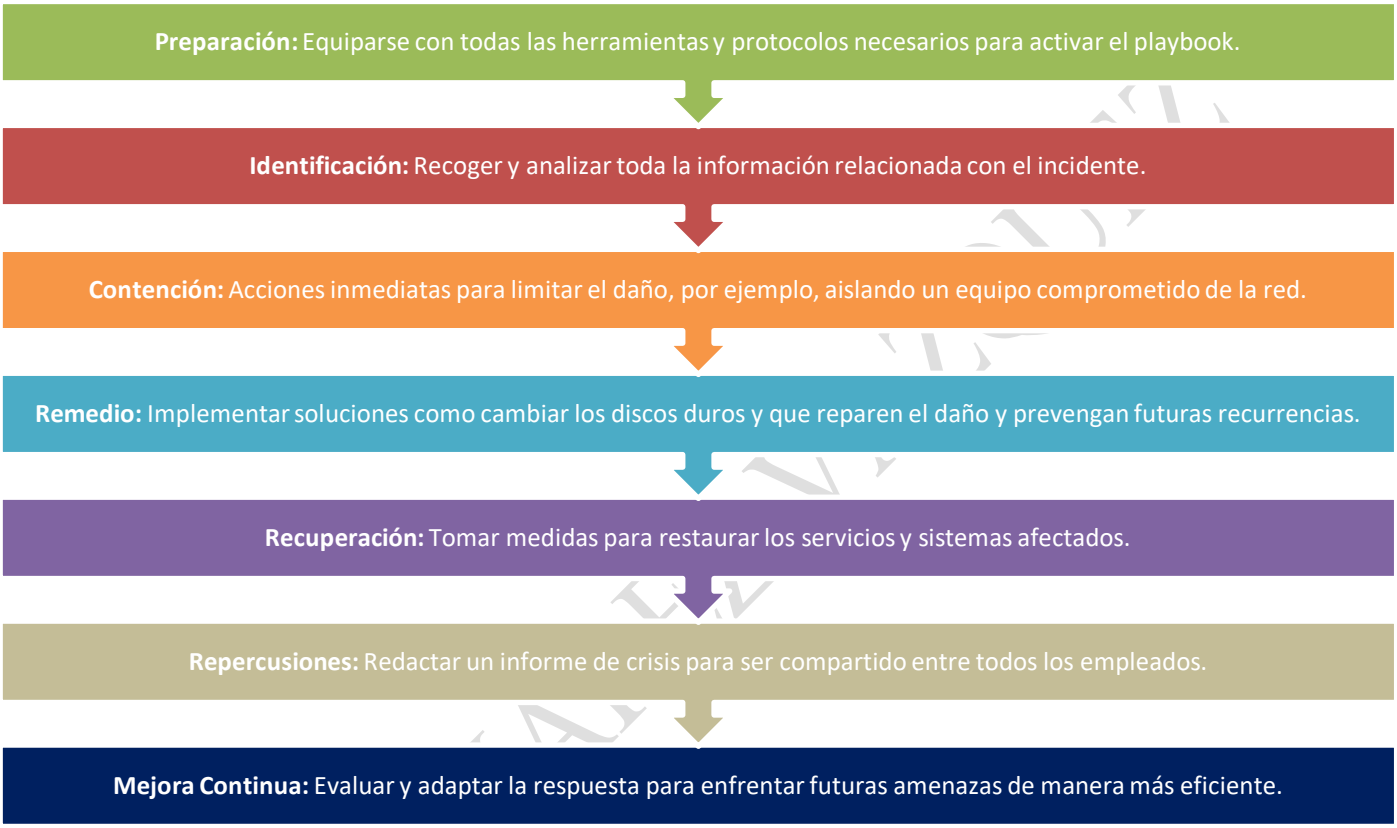
La **respuesta a incidentes** se refiere al **proceso** de **limpieza** y **recuperación** cuando se detecta una **violación** de **ciberseguridad**.

Es **fundamental** contar con un **plan** y un **equipo especializado** que se encargue de **gestionar** el **incidente**, con el **objetivo** de **minimizar daños** y **costos** de **recuperación**.

1.3. Objetivos y Fases del PlayBook general

El **principal** propósito de un **playbook** de respuesta a incidentes es **garantizar** que las empresas u organizaciones estén **preparadas** para enfrentar cualquier situación de **emergencia**. Es **esencial** que cada miembro esté **informado** y sepa qué hacer en caso de incidente, permitiendo así **minimizar impactos** y **resolver situaciones** de **manera rápida** y **eficaz**.

Estas son las **fases** de un **PlayBook** propuesto para incidentes de carácter general**:**



Las herramientas o procesos seguidos en cada paso son variables y cada empresa usará sus herramientas personales para ello.

1.4. ¿Sirven todos los PlayBook para cada empresa?

La respuesta depende en gran medida de la **matriz de riesgos** que contemple los **ciber-riesgos**, y que esté alineada con la **naturaleza** y **objetivos** de la **empresa**.
Es vital iniciar un **diálogo interno** y **definir estrategias** en **consonancia** con las **vulnerabilidades** y **amenazas específicas** de tu **sector.**

Si bien los **playbook** no **garantizan prevención** frente a **amenazas** inesperadas o nuevos tipos de ataques, sí **ofrecen** un **robusto** punto de partida para **prevenir** "decisiones impulsivas" en momentos de **crisis**.

Poseer un **protocolo** definido **potencia** las **respuestas** y **agiliza** los **tiempos** de acción. Un **gran error** es pensar que tu empresa es **inmune** a cualquier incidente. Tarde o temprano, estos sucesos pueden ocurrir.

La clave radica en cómo nos **preparamos** y **reaccionamos** ante ellos, y cómo nos **adaptamos basándonos** en lo aprendido.

1.5. Ventajas de tener un PlayBook

Mejora la Preparación: Un playbook fortalece la preparación de una empresa frente a incidentes o crisis, asegurando que cada integrante sepa exactamente cómo actuar en casos de emergencia, minimizando así el impacto y resolviendo el suceso eficientemente.

Reduce el Tiempo de Respuesta: Al contar con un playbook, se pueden activar protocolos de acción inmediatamente después de identificar un incidente, agilizando la solución y reduciendo el impacto en la organización.

Potencia la Comunicación: El playbook incluye un plan de comunicación que detalla la forma en que se deben notificar a empleados, clientes, garantizando que todos estén informados y puedan gestionar el suceso adecuadamente.

Aumenta la Confianza: Al contar con un playbook, se transmite un mensaje de preparación y profesionalismo a empleados y clientes, reforzando su confianza en la capacidad de la organización para manejar crisis.

Cumplimiento de Normativas: En algunos contextos, la ley puede requerir que las empresas tengan un plan de respuesta a incidentes. Tener un playbook garantiza el cumplimiento de estas regulaciones, evitando sanciones.

1.6. Fuentes de información

Fuentes contra ataques:

1. **FIRST (Forum of Incident Response and Security Teams)**
2. **SANS Institute**
3. **GitHub - Buscar playbooks de respuesta a incidentes**
4. **MITRE ATT&CK**
5. **CERT/CC**
6. **NIST - Computer Security Incident Handling Guide**
7. **CIS (Center for Internet Security)**
8. **Cybersecurity & Infrastructure Security Agency (CISA)**
9. **Incident Response Consortium**
10. **ENISA (European Union Agency for Cybersecurity)**

1.7. Ejemplo de PlayBook para un Ransomware

El **Instituto Nacional de Estándares y Tecnología (NIST)** y otras organizaciones como **INCIBE** proporcionan guías y **playbooks** para la **prevención**, **mitigación**, **protección** y **eliminación** de ataques de **ransomware**, así como para la recuperación y vuelta a la normalidad después de un ataque.
Sus fases se dividen en:

Prevención y Protección:

- Preparación: Las organizaciones deben **prepararse** para los ataques de **ransomware** **protegiendo** sus **datos** y **dispositivos**.
  Esto incluye mantener **actualizados** los **sistemas operativos** y **aplicaciones**, utilizar soluciones de seguridad efectivas como **firewalls** y **sistemas de detección** de **intrusiones**, y **educar** a los **usuarios** sobre las **amenazas** de **ransomware** y cómo **evitarlas**.

- Detección temprana: La **detección temprana** de **ransomware** requiere **diligencia** tanto de los **administradores** de sistemas como de los **usuarios**. Los indicadores de compromiso (**IOC**) son **fundamentales** para **identificar máquinas infectadas** o **actividad maliciosa**, permitiendo **responder rápidamente** a un **ataque**.

Mitigación y Eliminación:

- Respuesta inicial: En caso de detección de un ataque de **ransomware**, la **primera respuesta** debe incluir la **desconexión** de las **máquinas afectadas** de la red para **prevenir** la **propagación** del **malware**.
  También es crucial **comunicarse** con el equipo de **respuesta** a **incidentes** y **comenzar** a **recopilar datos forenses**.

- Erradicación: La **eliminación** del **ransomware** implica **identificar** y **aislar** las **máquinas infectadas**, realizar un inventario y **verificar** la **integridad** de todos los **sistemas** y **backups**, y proceder con la **limpieza** segura de los **sistemas infectados**.
  Es importante **seguir** las recomendaciones específicas del **playbook** de respuesta a incidentes de ransomware.

Recuperación y Vuelta a la Normalidad:

- Recuperación de datos: La **recuperación** de datos afectados por el **ransomware** puede realizarse a partir de **backups** que hayan sido **verificados** y que no estén **cifrados**. Es importante **restaurar** los sistemas desde estos **backups** y asegurarse de que los sistemas y cuentas de usuario estén **protegidos** adecuadamente.

- Revisión y mejora de la seguridad: Después de la **recuperación**, es **fundamental** revisar y **mejorar** las **medidas** de **seguridad** para prevenir **futuros ataques**. Esto incluye **fortalecer** las **políticas** de **seguridad**, realizar **pruebas** de **penetración** y **ejercicios** de **respuesta** a **incidentes**, y **mantenerse** al día con las **últimas amenazas** y **vulnerabilidades**.

Conclusión:

- La **prevención**, **mitigación**, **protección** y **eliminación** de ataques de **ransomware**, así como la **recuperación** y **vuelta** a la **normalidad**, requieren un **enfoque estructurado** y **colaborativo** entre diferentes **equipos** dentro de una **organización o empresa**.

- Utilizar **playbooks** y **guías** como las **proporcionadas** por **NIST** e **INCIBE** puede ayudar **significativamente** a las **organizaciones** a **prepararse** y **responder** eficazmente a estos **ataques**.

Enlaces de ayuda:

- **https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware**
- **https://csrc.nist.gov/projects/ransomware-protection-and-response**
- **https://download.microsoft.com/download/3/d/d/3ddd4682-6764-4738-a12f-6710cbdddc64/Ransomware%20Incident%20Response%20Playbook%20Template.pdf**
- **https://nmfta.org/wp-content/media/2022/11/Ransomware-Playbook-Template.pdf**
- **https://www.cisa.gov/stopransomware/ive-been-hit-ransomware**
- **https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf**
- **https://github.com/certsocietegenerale/IRM/blob/main/EN/IRM-17-Ransomware.pdf**
- **https://www.incibe.es/aprendeciberseguridad/ransomware**
- **https://www.incibe.es/incibe-cert/blog/enfrentandonosransomware**

2. Ciberresilencia a Incidentes

2.1. ¿Qué es?

La capacidad de **ciberresiliencia** ante incidentes se refiere a la **habilidad** de una empresa u organización para **resistir** y/o **recuperarse** ante **ataques** o **incidentes cibernéticos**.
Esta capacidad implica una serie de **estrategias** y **tecnologías** diseñadas para **anticipar** posibles **ataques**, **detectarlos** de manera temprana y **proporcionar** una **respuesta rápida** que permita **recuperarse** y **continuar** con las actividades normales.

La **ciberresiliencia** es esencial para proteger los activos digitales y la **continuidad** de los sistemas frente a **ciberataques**.

2.2. ¿Cómo pueden las empresas conseguirlo?

Para **desarrollar** la **ciberresiliencia**, las empresas deben **enfrentar** varios **desafíos**, como la **escasez** de **habilidades** o **formación** en **ciberseguridad** y la **necesidad** de comprender **profundamente** sus propios **sistemas**, que están en constante **evolución**.
Por lo tanto, es crucial **contar** con el **apoyo** de **expertos** y **profesionales** en **ciberseguridad** para implementar eficazmente la **ciberresiliencia** y **adaptarse** a las situaciones de **riesgo** que puedan surgir.

Además implementar la **ciberresiliencia** implica **preparar** los **sistemas** y las **políticas** de actuación frente a las **ciberamenazas** actuales.
Esto incluye **prever posibles escenarios** de compromiso, **evaluar** la **probabilidad** de **compromisos**, **entender** la **posible ruta** de **propagación** y **planificar** la **respuesta** adecuada.

Fuentes:

- https://www.incibe.es/incibe-cert/blog/ciberresiliencia-la-clave-para-sobreponerse-los-incidentes
- https://s2grupo.es/que-es-la-ciberresiliencia-y-por-que-es-importante-para-las-empresas/#:~:text=La%20ciberresiliencia%20(a%20veces%20denominada,ante%20ataques%20o%20incidentes%20cibern%C3%A9ticos.
- https://www.docusign.com/es-mx/blog/ciberresiliencia
- https://www.ikusi.com/mx/blog/ciberresiliencia/

3. Flujo de tomas de decisiones

Establecer un **flujo de toma de decisiones** y **escalado** de **incidentes** interno y/o externo adecuado es fundamental para gestionar **eficazmente** cualquier evento de seguridad o **ciberataque.**

Este **proceso** permite a las **empresas responder** de **manera rápida**, **eficiente** y **coordinada** a las amenazas, **minimizando** el **impacto**.

Sus ventajas son:

https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

4. Tareas de Restablecimiento y Vuelta a la Normalidad

4.1. Pasos durante el incidente

Contención
- Se detiene la propagación del ransomware en la red. Esto puede implicar desconectar las máquinas infectadas de la red, bloquear puertos específicos o desactivar servicios que podrían estar siendo utilizados por el ransomware

Erradicación
- Se elimina completamente el ransomware de todos los sistemas afectados. Esto puede requerir el uso de herramientas especializadas y la realización de pruebas exhaustivas para asegurar que el malware ha sido completamente eliminado

Recuperación
- Se restauran los sistemas y datos afectados a su estado normal. Esto puede implicar la restauración de sistemas desde copias de seguridad, la reparación de archivos dañados y la reconfiguración de sistemas afectados.

4.2 Pasos tras el Incidente

Análisis Post-Incidente
- Se realiza un análisis detallado del incidente para entender cómo ocurrió, identificar las vulnerabilidades que permitieron el ataque y aprender de la experiencia. Esto puede incluir la revisión de registros de eventos, la realización de pruebas de penetración y la revisión de las políticas de seguridad existentes.

Mejora de la Seguridad
- Basándose en los hallazgos del análisis post-incidente, se implementan mejoras en las medidas de seguridad de la organización. Esto puede incluir la actualización de sistemas y software, la implementación de nuevas políticas de seguridad y la capacitación de personal en mejores prácticas de seguridad.

Pruebas de Resiliencia
- Se realizan pruebas de resiliencia para asegurar que la organización puede responder eficazmente a futuros incidentes. Esto puede incluir pruebas de penetración, simulacros de incidentes y la evaluación de la capacidad de respuesta de la organización.

Monitoreo Continuo
- Se mantiene un monitoreo continuo de la red y los sistemas para detectar cualquier actividad sospechosa o signos de reinfección. Esto es vital para asegurar que la organización esté preparada para responder rápidamente a futuros ataques.

5. Registro de lecciones aprendidas

5.1. Acciones realizadas

Documentación Detallada: Registrar todos los aspectos del incidente, incluyendo la fecha, hora, sistemas afectados, impacto, medidas tomadas para contener y erradicar el incidente

Análisis Forense: Realizar un análisis forense de los sistemas afectados para entender cómo se infiltró el ataque, qué sistemas fueron comprometidos y cómo se propagó el incidente.

Revisión de Políticas y Procedimientos: Evaluar las políticas y procedimientos de seguridad existentes para determinar si fallaron en algún punto durante el incidente

Simulacros y Pruebas de Penetración: Después de la revisión, realizar simulacros y pruebas de penetración para probar la eficacia de las medidas de seguridad añadidas

5.2. Conclusiones aprendidas

Identificación de Vulnerabilidades: Basándose en el análisis forense y la revisión de políticas, identificar las vulnerabilidades que permitieron el incidente

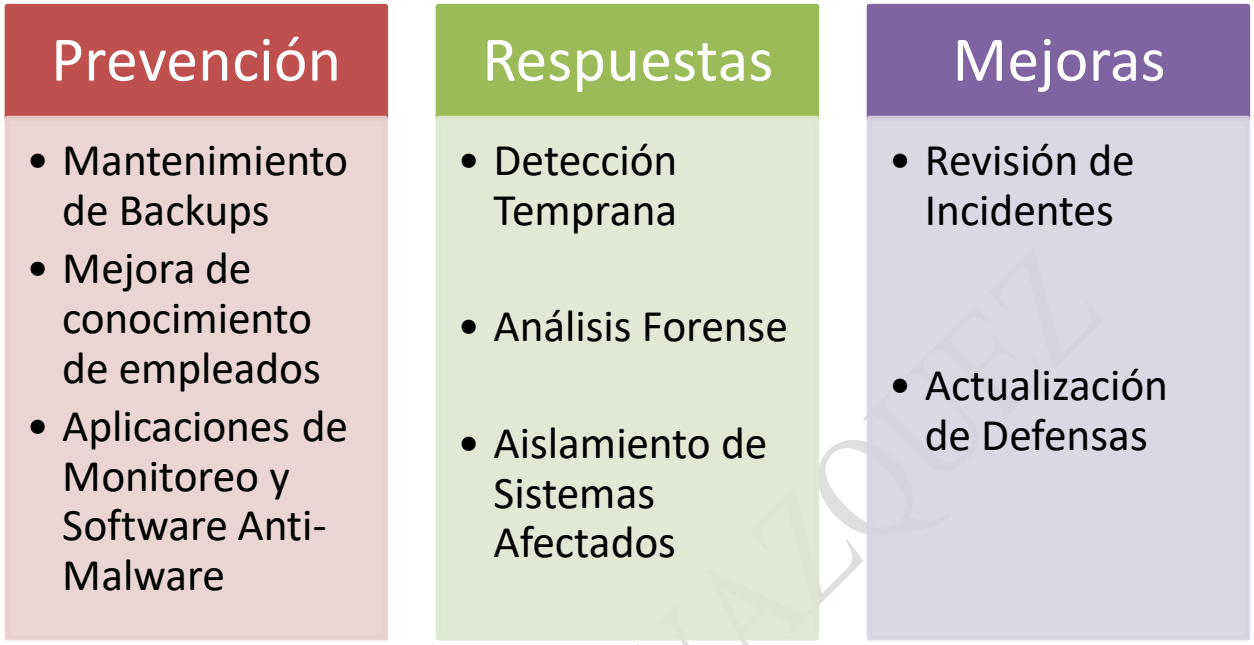
Mejoras en Procedimientos: Implementar cambios en los procedimientos de seguridad para cerrar las brechas identificadas

Plan de Respuesta Mejorado: Incorporar las lecciones aprendidas en el plan de respuesta a incidentes y en el programa general de gestión de la seguridad.

Cultura de Seguridad: Fomentar una cultura de seguridad en la organización, donde todos los miembros del equipo estén conscientes de la importancia de la seguridad

6. Protecciones para evitar esta situación de nuevo

6.1. Acciones a realizar

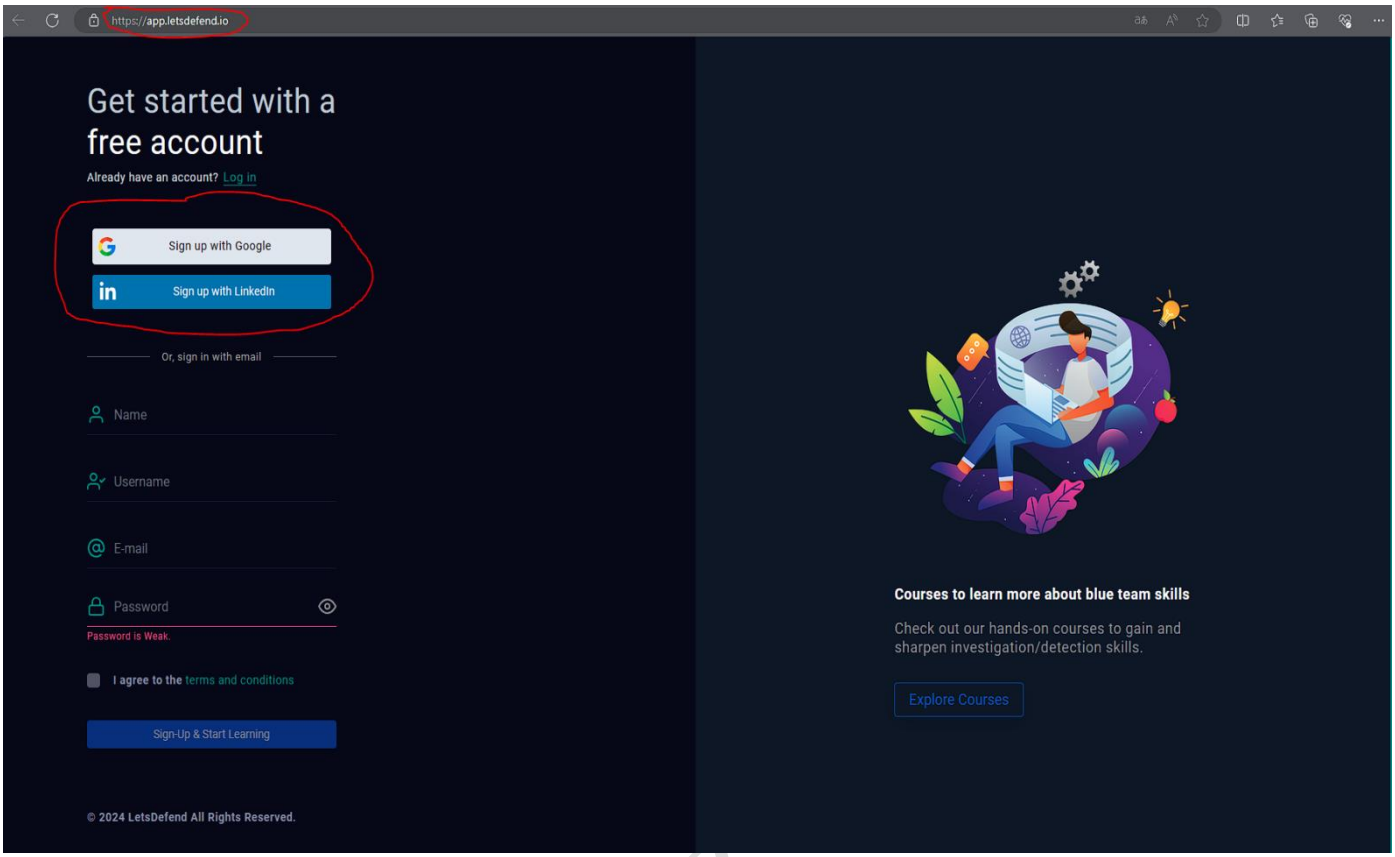


6.2. Plataforma LetsDefend

La plataforma **LetsDefend (**https://app.letsdefend.io/) ofrece **cursos** prácticos diseñados para **mejorar** las **habilidades** de **investigación** y **detección** en el contexto del seguimiento de **incidentes**. Estos cursos están dirigidos a los miembros del **equipo azul (blue team)**, quienes son responsables de la **defensa** y la **respuesta** a **incidentes** en las empresas.
La utilidad de LetsDefend en el seguimiento de incidentes radica en:

- Fortalecimiento de Habilidades: Los **cursos** de **LetsDefend** están diseñados para **enseñar** y **perfeccionar habilidades** específicas relacionadas con la **investigación** y **detección** de **incidentes**.
- Aprendizaje Aplicado: La **plataforma** se destaca por ofrecer un **enfoque práctico** en el aprendizaje, lo que significa que los participantes tienen la **oportunidad** de aplicar lo que aprenden en situaciones **reales** o **simuladas**.
- Acceso a Recursos Específicos: LetsDefend proporciona a los usuarios **acceso** a **recursos** y **herramientas especializadas** que pueden ser **difíciles** de encontrar en otros lugares o plataformas.

LetsDefend es una plataforma valiosa para el **seguimiento de incidentes** debido a su enfoque en el **desarrollo de habilidades prácticas** y su **acceso** a **recursos especializados**.



VideoTutorial de la demo de LetsDefend:
[Letsdefend Walkthrough demo (youtube.com)]

6.3. Herramientas de Seguimiento

- **Jira (https://www.atlassian.com/es/software/jira)**

Jira es una herramienta de **seguimiento** de **incidencias** y **administración** de **proyectos** que permite a los equipos **gestionar** y **priorizar** el **trabajo** de manera eficiente.
Jira es especialmente útil para equipos que trabajan con **metodologías ágiles** como **Scrum** y **Kanban**, ya que facilita la planificación de **sprints** y la visualización del **progreso** del **trabajo**.

La integración de **Playbooks** en **Jira** es posible debido a su **flexibilidad** y **capacidad** para **adaptarse** a diferentes flujos de trabajo. Los **Playbooks** pueden ser utilizados para definir **procedimientos estándar** o **respuestas predefinidas** a ciertos **tipos** de **incidentes**, lo que ayuda a **acelerar** la **resolución** de **problemas** y **mejora** la **consistencia** en la **gestión** de **incidentes**.

- **Witei (https://get.witei.com/es/)**

Witei es una solución que integra un **gestor de incidencias** dentro de su **CRM** (**Customer Relationship Management** diseñado para ventas, marketing y atención al cliente), permitiendo a los **usuarios** realizar un **seguimiento integral** de lo que ocurre con todos sus contactos **registrados** en el **CRM**.
Esto incluye ver el **historial** del **cliente**, todas las **conversaciones** que se han mantenido con él, su **información**, asignar las **fichas** al **empleado** que corresponda, dar una **prioridad** a cada **ticket**, indicar el estado del **incidente**, y conocer la **satisfacción conseguida** por el **cliente**.

Además, este sistema facilita la **comunicación interna** entre los **trabajadores** y otra **pública** con el **cliente**, permitiendo atender la **incidencia** desde un único **lugar** y desde cualquier sitio gracias a su diseño **responsive**.

La posibilidad de integrar **Playbooks** en herramientas como **Witei** es crucial para asegurar que los equipos sigan **procedimientos estandarizados** y **respondan** de manera coherente a las **solicitudes** de **servicio** o **incidentes**, esto no solo **mejora** la **eficiencia** en la resolución de **problemas** sino que también garantiza una **experiencia** de usuario consistente.
La integración de **Playbooks** facilita la **adopción** de **buenas prácticas**, **mejora la calidad** del **servicio** y **reduce** el **tiempo necesario** para resolver **incidentes**, lo cual es **esencial** para mantener la **disponibilidad** y la **satisfacción** del **cliente.**